REMARKS

The Office Action dated May 6, 2004 has been received and carefully considered. In this response, claims 1 and 7 have been amended and claims 6, 8, 9, 21-23, 33 and 34 have been canceled without prejudice. The amendments to claims 1 and 7 do not narrow the scope of the claims and no new matter is introduced by these amendments. Reconsideration of the outstanding rejections in the present application therefore is respectfully requested based on the following remarks.

Indefinite and Enablement Rejections of Claims 6, 8, 9, 21-23, 33 and 34

At page 2 of the Office Action, claims 6, 8, 9, 21-23, 33 and 34 were rejected under 35 U.S.C. § 112, second paragraph, as being indefinite. At page 5 of the Office Action, claims 6, 8, 9, 21-23, 33 and 34 were rejected under 35 U.S.C. § 112, first paragraph, as being failing to comply with the enablement requirement. Claims 6, 8, 9, 21-23, 33 and 34 have been canceled without prejudice, thereby obviating this rejection. Accordingly, the Applicant respectfully submits that the rejections of claims 6, 8, 9, 21-23, 33 and 34 are improper at this time and withdrawal of these rejections therefore is respectfully requested.

Anticipation Rejection of Claims 1-9, 12-16 and 21-23

At page 6 of the Office Action, claims 1-9, 12-16 and 21-23 were rejected under 35 U.S.C. § 102(a) as being anticipated by Patel (U.S. Patent No. 6,243,811). This rejection is respectfully traversed.

At the outset, the Applicant respectfully submits that Patel does not qualify as prior art under 35 U.S.C. § 102(a), which provides that an invention is not patentable if "the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, *before invention thereof* by the applicant for a patent." (emphasis added). The present application was filed on September 26, 2000 and Patel published on June 5, 2001, so the disclosure of Patel cannot be considered as "described in a printed publication . . . before" the invention of the present application. However, in the interest of advancing the

present application, the Applicant provides the following remarks under the assumption that Patel provisionally qualifies as prior art under 35 U.S.C. § 102(e).

Claim 1, from which claims 2-5, 7 and 10-13 depend, recites, in part, the limitations of providing a first seed key and a public encryption key associated with a peripheral device to a hardware controller and generating at the hardware controller, *using the first seed key and the public encryption key*, a second seed key different from the first seed key, *the second seed key to encrypt communications between the software component and the hardware controller*. Claim 14, from which claims 15-20 depend, recites similar limitations. The Examiner asserts that Patel discloses these limitations and cites the passages at col. 1, lines 55-64, col. 2, lines 55-59, and col. 4, lines 1-11 of Patel in support of this assertion. For ease of reference, these passages are reproduced in full below:

> A root key, known as the A-key, is stored only in the AC/HLR 10 and the mobile 20. There is a secondary key, known as Shared Secret Data SSD, which is sent to the VLR 15 as the mobile roams (i.e., when the mobile is outside its home coverage area) . *SSD is generated from the A-key and a random seed RANDSSD using a cryptographic algorithm or function.* A cryptographic function is a function which generates an output having a predetermined number of bits based on a range of possible inputs.

Patel, col. 1, lines 55-64 (emphasis added).

> The random numbers R_M and R_N are referred to as challenges, while $CAVE_{SSDA}(R_M)$ and $CAVE_{SSDA}(R_N)$ are referred to as challenge responses. Once the authentication is complete, the mobile 20 and the network generate session keys using SSDB.

Patel, col. 2, lines 55-59.

> In the method according to the present invention, however, the AC/HLR 10 and the mobile 20 also generate another key, referred to as the M-key, based on the root or A-key. For example, the M-key is generated by applying a pseudo random function (PRF) indexed by the A-key on a known value. A practical PRF is the well-known Data Encryption Standard-Cipher Block Chaining (DES-CBC) from the NIST (National Institute of Standards). In a preferred embodiment, DES-CBC, indexed by a 64-bit A-key on a value known to both the network and the mobile 20, produces a 64-bit M-key.

Patel, col. 2, lines 55-59.

The Applicant respectfully submits that the Office Action fails to establish that the cited

passages of Patel disclose or suggest the limitations of generating of a second key, using a first seed key and a public encryption key as recited in claims 1 and 14. The Examiner appears to equate the SSD of Patel to the second seed key, the M-key of Patel to the first seed key and the A-key to the public encryption key. Office Action, p. 6-7. The Applicant objects to the Examiner's characterization of the A-key of Patel as a public encryption key. One of ordinary skill in the art will recognize that a public encryption key is one encryption key of a key pair that may be provided via non-secure means (i.e., "publicly") since the public encryption key is used only to encrypt information, but cannot be used to decrypt that same information. In contrast, Patel teaches that the A-key is "stored only in the AC/HLR 10 and the mobile 20." As the A-key is limited to only the HLR 10 and the mobile 20, the A-key does not qualify as a public encryption key. Moreover, the Examiner errs in asserting that Patel discloses the generation of the SSD from the A-key and the M-key. *Id.*, p. 7. As recited by Patel at col. 2, lines 60-62, the "SSD is generated from the A-key and a random seed RANDSSD," instead of from a public encryption key. As with the A-key of Patel, the random seed RANDSSD is not a public encryption key as it is generated pseudo-randomly and therefore does not have a cryptological relation to a private encryption key. The Applicant also respectfully submits that Patel fails to disclose or suggest that the SSD is used to encrypt communications as recited in claims 1 and 14. Instead, Patel teaches using the SSD for authentication purposes. *See, e.g., Patel*, col. 2, lines 59-60 (teaching that the SSD is used to "answer the challenges from the mobile 20 and the network").

In addition, it is respectfully submitted that the Office Action fails to establish that the cited passages of Patel disclose or suggest the limitations of providing a first seed key and a public encryption key associated with a peripheral device to a hardware controller as recited by claims 1 and 14. While the Examiner asserts that the passage at col. 4, lines 1-11 of Patel disclose these limitations, the Applicant is unable to discern any disclosure in this passage related to providing keys to any device, much less a hardware controller. Moreover, in asserting that Patel discloses these limitations, the Examiner erroneously equates the A-key of Patel to a public encryption key (as discussed above).

Accordingly, since Patel fails to disclose at least the limitations of providing a first seed key and a public encryption key associated with a peripheral device to a hardware controller,

generating a second key using a first seed key and a public encryption key, or using the second key to encrypt communications as recited in claims 1 and 14, the Applicant respectfully submits that the Office Action fails to establish that Patel discloses or even suggests each and every limitation of claims 1 and 14. Consequently, the Office Action fails to establish that Patel discloses or suggests each and every limitation of claims 2-5, 7, 10-13 and 15-20 at least by virtue of their dependency from one of claims 1 or 14. Moreover, these claims recite additional limitations that are not disclosed by Patel. For example, claims 3 and 15 recite the limitations of using a public encryption key associated with a peripheral device to select a plurality of private encryption keys associated with a software component and determining a seed key based on the selected private keys. The Applicant respectfully submits that Patel also fails to disclose these limitations.

In view of the foregoing, the Applicant respectfully submits the anticipation rejection of claims 1-9, 12-16 and 21-23 is improper at this time and the withdrawal of this rejection therefore is respectfully requested.

Obviousness Rejection of Claims 10, 11, 17-20 and 24-35

At page 12 of the Office Action, claims 10, 11, 17-20 and 24-35 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Patel. This rejection is respectfully traversed.

Claims 1, from which claims 10 and 11 depend, and claim 14, from which claims 17-20 depend, recite, in part, the limitations of providing a first seed key and a public encryption key associated with a peripheral device to a hardware controller and generating a second key using a first seed key and a public encryption key, where the second key is used to encrypt communications. Claim 24, from which claims 25-32 and 35 depend, recites similar limitations. As discussed above, Patel fails to disclose at least these limitations. Accordingly, Patel fails to disclose each and every limitation of claims 10, 11, 17-20, 25-32 and 35 at least by virtue of their dependency from one of claims 1, 14 and 24. Moreover, these claims recite additional limitations that are non-obvious in view of Patel.

Accordingly, the Applicant respectfully submits the obviousness rejection of claims 10, 11, 17-20 and 24-35 is improper at this time and the withdrawal of this rejection therefore is respectfully requested.

Conclusion

It is respectfully submitted that the present application is in condition for allowance and an early indication of the same is courteously solicited. The Examiner is respectfully requested to contact the undersigned by telephone at the below listed telephone number in order to expedite resolution of any issues and to expedite passage of the present application to issue, if any comments, questions, or suggestions arise in connection with the present application.

The Applicant do not believe that any additional fees are due, but if the Commissioner believes additional fees are due, the Commissioner is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 50-0441.

Respectfully submitted,

August 2, 2004
Date

Ryan S. Davidson, Reg. No. 51,596
On Behalf Of
J. Gustav Larson, Reg. No. 39,263
Attorney for Applicant
TOLER, LARSON & ABEL, L.L.P.
5000 Plaza On The Lake, Suite 265
Austin, Texas 78746
(512) 327-5515 (phone)
(512) 327-5452 (fax)